*Current Journal of Applied Science and Technology*

***40(14): 10-19, 2021; Article no.CJAST.69679***
***ISSN: 2457-1024***
*(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843, NLM ID: 101664541)*

# Computer Security Practices in Senior High Schools in the Keta Municipality

**Abraham Tetteh[1*], Richard Essah[2], Gifty Opoku[3] and Monica Akua Serwaa[4]**

*[1]Bia Lamplighter College of Education, P.O.Box 97, Sefwi-Debiso, Ghana.*
*[2]Chandigarh University, Punjab-140413, India.*
*[3]St. Louis Senior High School, P.O.Box 11, Amekom – Kumasi, Ghana.*
*[4]St. George Catholic Senior High Technical School, P.O.Box 7104, Adum-Kumasi, Ghana.*

***Authors' contributions***

*This work was carried out in collaboration among all authors. Author AT designed the study, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript. Authors RE and MAS managed the analyses of the study. Author GO managed the literature searches. All authors read and approved the final manuscript.*

***Article Information***

DOI: 10.9734/CJAST/2021/v40i1431398
Editor(s):
(1) Dr. Orlando Manuel da Costa Gomes, Lisbon Polytechnic Institute, Portugal.
Reviewers:
(1) David Adeola Akinwumi, Adekunle Ajasin University, Nigeria.
(2) Carrie Carmody, California State University, USA.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69679

***Original Research Article***

***Received 10 April 2021***
***Accepted 14 June 2021***
***Published 19 June 2021***

## ABSTRACT

**Aims:** To examine security practices in Senior High Schools in Keta Municicpality.
**Study design:** Descriptive Survey Design.
**Place and duration of study:** The study was undertaken in the Keta Municipality of Volta Region.
**Methodology:** The researcher adopted quantitative research design. The target population for the study was made up of eight (8) senior high schools with four thousand two hundred (4200) senior high school students, teachers, administrators and account clerks in the Municipality. The total number of samples for the study was hundred (100) respondents. This comprises forty (40) teachers, forty (40) students, ten (10) ICT teachers, five (5) administrators and five (5) account clerks all from the five selected schools. The research instrument used for the data collection was questionnaire. The usage of a data analysis application known as the International Business Machine, Statistical Package for Social Sciences, assisted the data analysis (IBM SPSS).
**Results:** The results revealed that 35(87.5%) of students agreed to the fact that they used computer with permission, 32(64%) of teachers emphasized that there were security passwords on computers in their schools, and 27(82.5%) of students indicated that there are codes of conduct guiding

**Corresponding author: E-mail: abrahamtetteh@blce.edu.gh;*

computer usage in their schools. However, 20(40%) of teachers emphasized that intrusion detective system was not used on computers in their schools to detect network attack and that 7(70%) of administrators and account clerks attested to the fact that Antivirus is installed on computers in my school

**Conclusion:** Many schools in the Keta Municipality do not have enough computers let alone sustainable power generation in the schools and this has affected effective teaching and learning and quality education delivering.

*Keywords: Computer; security; teachers; students; administrator; account clerk; senior high school.*

## 1. INTRODUCTION

The usage of the Internet is rapidly increasing over the world [1]; according to a December 2010 estimate, there are around 6,845 million Internet users globally. However, this expansion is accompanied with dangers, particularly the distributed denial-of-service assault, which renders the target unable to provide normal service [2]. This is a threat to the secrecy, authentication, integrity, nonrepudiation, access control, and availability of computer networks [3]. The main goal of these attacks is to prevent the user from properly accessing the resource or service. Information about attacks on computers cannot only be important for users but also can cause those users a difficult task to link to the internet connection [4]. Therefore, there is the need for educational institutions to practice computer security to avoid the disadvantages that may arise from computer threat and attack [5].

Computer security is an activity, equipment, procedure, or technique that reduces a threat, vulnerability, or assault by removing or avoiding it and minimizing the harm it can cause, or by identifying and reporting it so that remedial action can be performed [6]. Computer security isn't quite new, but it has reawakened attention in recent years as a result of the failure of network-based security measures such as firewalls. Unfortunately, today's software has design bugs as well as implementation defects, posing an intolerable security risk [7]. Any application, no matter how harmless it appears, might include security flaws. Despite the fact that the concept of computer security risk has been widely accepted, developers, architects, and computer scientists have only recently began to investigate how to create secure software [8]. Essentially, money spent by users on network, computer security, and other perimeter solutions is not resolving computer security issues. In the scientific community, a body of computer security literature has begun to form, but in reality, computer security is still in its infancy. For example, the first books on computer security and security engineering were just released [9,2]. A number of references already exist that provide a philosophical foundation for computer security as well as examination of specific technological concerns, but considerable work remains to be done to put computer security into practice [10].

However, computer security practice is a serious issue affecting effective teaching and learning and school management in senior high schools in Ghana in general and the Keta Municipality in particular and indeed need a pragmatic and urgent attention. According to Klein, Roffi, and Hehir [11], computer security enables schools and institutions to fulfill their mission by allowing people to do their jobs, educate themselves, and conduct research while also supporting critical business processes and protecting personal data and sensitive information. This means that everybody who uses a computer or a mobile device must be aware of how to keep their computer, device, and data safe. Everyone is responsible for information technology security. Computer security practices should therefore be enforced and applied in senior high schools in the Keta Municipality if indeed security and protection of school's data and information are taken serious.

Understanding software-induced security vulnerabilities and how to address them is important to computer security [10]. Good computer security practice is based on good computer engineering practice and entails considering security early in the software development lifecycle. This aids in the recognition and comprehension of common issues such as language-based defects, pitfalls, designing for security, and exposing all software products to objective risk evaluations and testing [12]. Therefore, there is the need to institute computer security intelligent practices everywhere especially in senior high schools. There should be intrusion detective system to

alert users or networks that are under attack but majority of senior high schools in the Keta Municipality lack computer security practices and pose a serious threat to computers and networks. People are more interested in other applications, although in many ways computer security should be a natural domain of application for artificial intelligent (AI) [13]. Many senior high schools operate ICT tools and equipment without instituting any measures to protect and prevent piracy activities and hijackers of computer system. Some of the senior high schools in the Keta Municipality do not comply and adhere to any computer security practices, let alone have antivirus to protect computer hardware and software especially computer and its accessories therefore subject files to virus attack. Most of computers in senior high schools in the Keta Municipality do not have secure measures and therefore makes it possible for pirates to break intellectual property laws by copy bootleggers, producing protected works and copyright works without permission. Pirates and hijackers seize the control of networked computers by means of infecting them with a worm and other malwares thereby turning them into a zombie [14]. These groups of people change software settings without users' knowledge so as to force the users to visit certain website.

They introduced an amendment deleting the contents of bills, documents and inserting entirely new provisions [15]. All these activities organised by the hijackers and pirates undermine and hinder successful use of computers and networks in senior high schools in the Keta Municipality. The cyber-attack on computer systems and networks indeed has to be minimised and reduced to the barest minimum by using intrusion detective system to protect files [16], documents, personnel records, leakage of examination questions, change of examination results, duplication of files, vital property and document of the schools from being hijacked and leaked to the public. As a result, the study sought to identify the trends of computer security practices in senior high schools in the Keta Municipality. The findings of the study will assist ICT teachers, headmasters and school account clerks to identify the need to use detective system in computer operative system and networks in order to avoid security breaches in their schools. The study will inform school management to develop computer network security to prevent attack on confidentiality, authentication, integrity, nonrepudiation, access control, and availability. The study will be more beneficial to West Africa Examination Council to use detective mechanisms and instruments to protect the safety of examination questions and certificates.

## 2. METHODOLOGY

The researcher adopted quantitative research design and it is a process in which numerical data is used to obtain information and consist of descriptive, correlational, experimental and quasi-experimental research. The descriptive survey was the main focus of this study and is the exploration and description of phenomena in real life situation. The study was undertaken in the Keta Municipality of Volta Region. The target population for the study was made up of one (1) senior high school with one thousand one hundred (1100) senior high school students, teachers, administrators and account clerks in the Municipality. Three hundred and forty-eight (48) teachers, one (1) headmaster, ten (10) administrators and account clerks as well as one (1) bursar for the municipality were also covered in the study.

### 2.1 Sampling Technique

Random sampling and purposive sampling techniques were employed to select the representative of the study. A random sampling strategy was used to select a representative number of one (1), school for the study due to the nature and the use of descriptive survey. The school was Anlo Afiadenyigba senior High School (A). The study was limited to senior high school since participants were matured as compared to the junior high school students and as such are capable of responding to the items on the questionnaire and structured interview schedule appropriately and responsibly. In the case of the teachers, eight (8) individuals were blindfolded and asked to pick a piece of paper inscription 'participant' and 'non-participant' from a basket. This method was used and applied in the school and as such forty (40) teachers were selected. As in case of students eight (8) individuals were also blindfolded and asked to pick a piece of paper inscription 'participant' and 'non-participant' from a basket. This same procedure was used and applied in the school and as such forty (40) students were chosen. The views of ICT teachers were also sought. In this case all individuals were selected. Ten (10) ICT teachers were selected as a result. Random sampling technique was appropriate, simple and adopted since it established homogeneity.

Purposive sampling is a sampling approach in which researchers choose individuals and locations with the purpose of learning about or understanding the central phenomenon [17]. Purposive sampling was employed to select the administrators and account clerks of five schools mentioned. Purposive sampling was chosen because the respondents involved were single individuals who can be hand-picked based on the purpose of the study. Purposive sampling was used to select ten (10) administrator and an account clerk from the school. These individual respondents were selected and used to verify and cross- check responses on computer security practices in selected senior schools in Keta Municipality. The issue of triangulation in relation to the responses is ensured. The total number of samples for the study was hundred (100) respondents. This comprises forty (40) teachers, forty (40) students, ten (10) ICT teachers, five (5) administrators and five (5) account clerks all from the five selected schools.

## 2.2 Materials

The research instrument used for the data collection was questionnaires for the teachers, students, administrators and account clerks. There were thirty-two (32) items in the questionnaire for students. Questionnaire for students was made to examine the trend of computer security practices in senior high schools. There were thirty-nine (39) items in the questionnaire for both teachers and ICT teachers. Questionnaire for teachers was made to examine the trend of computer security practices in senior high schools. In addition, thirty-four (34) items were in the questionnaire for administrators and account clerks. The questionnaire examines trends of computer security practices in Senior High School students. The questionnaire was arranged in 5-point Likert scale with Strongly Agree = 1, Agree = 2, Neutral = 3, Disagree = 4 and Strongly Disagree = 5.

## 2.3 Data Collection Procedure

The researcher visited the selected senior high schools personally with a letter to seek permission from the headmasters as well as the cooperation of teachers, students, administrators and account clerks in order to gather the required and the necessary data for the study. Being a teacher in the municipality, it was very easy to gain the support and participation of all concerned. After consultation with the respondents, agreed dates were scheduled and all were informed about the dates and the purpose of the questionnaires they were to complete. The researcher went to the selected schools on the said dates and administered the questionnaires. Teachers, students, administrators and account clerks were enlightened on how to respond to the items. All questionnaires were examined and clarification made were necessary before collection.

## 2.4 Data Analysis

The statistical technique used for the study was descriptive statistics and this was primarily employed for the data analysis. The data obtained were computed and analysed using percentages and frequencies. The usage of a data analysis application known as the International Business Machine, Statistical Package for Social Sciences, assisted the data analysis (IBM SPSS). The respondents' responses were counted, frequencies were recorded, and a frequency distribution table was created using the data. The frequencies were transformed into percentages, which assisted in determining the various responses provided by different proportions of the study sample.

## 2.5 Ethical Consideration

The purpose of the study was not to intrude on people's privacy. Permission was requested from appropriate supporting heads and respondents associated with the study to deal with ethical issues linked with it. The study's goal was briefly described to them, and they were given the opportunity to select whether or not they wanted to participate. The information gathered was likewise kept in tight confidence, with anonymity and privacy guaranteed.

# 3. RESULTS AND DISCUSSION

The participants were asked to rate how much they agreed or disagreed with each of a series of statements. There were five response categories for each scale item, ranging from strongly agree to strongly disagree. The description given in text on “agree” is based on the total number and percentage that responded ‘strongly agree’ plus those who responded to ‘agree’ while those who responded to ‘disagree’ plus those who responded to ‘strongly disagree’ are together termed as “disagree” and then ‘neutral’ for those who have no knowledge of the question to respond. This section comprises of Tables 1, 2

and 3 and they establish the various trends of computer security practices by the students, teachers, Administrators and Account Clerks in the various Senior High schools in the Keta Municipality. It brings to bear some of the security practices that are practiced in schools.

Table 1 shows that 35(87.5%) of respondents agreed to the fact that they used computer with permission. The data above established that students did not use computers anyhow in all senior high schools in the Keta Municipality especially school that have computers. Also, it been established in Table 1 that majority 19(47.5%) of respondents attested to the fact that there is password on computers in their schools whilst only 17(43.0%) of respondents disagreed. This clearly indicated that computer security practices were strictly followed in some of the senior high schools in the Keta Municipality. Data in Table 1 reveals that 27(82.5%) of respondents indicated that there are codes of conduct guiding computer usage in their schools and 5(12.5%) disagreed which indicates that a good percentage of schools educate their students on what to do and what not to do when with the computers. Also, it been established in Table 1 that majority 29(72.5%) of respondents attested to the fact that network security protocols are enforced in the school whilst only 11(26.5%) of respondents disagreed. This clearly indicated that network security protocols are enforced in some of the senior high schools in the Keta Municipality. Also, it been established in Table 1 that majority 24(60%) of respondents attested to the fact that computers are used for 70% during teaching and learning in the school whilst only 16(40%) of respondents disagreed. This clearly indicated that computers are used for 70% during teaching and learning in some of the senior high schools in the Keta Municipality. Also, it been established in Table 1 that majority 39(92.5%) of respondents attested to the fact that there is no hacking attacks occuring with the computers in the school whilst only 1(2.5%) of respondents chose neutral. This clearly indicated that there is no hacking attacks occuring with the computers in some of the senior high schools in the Keta Municipality.

Table 2 indicates that majority 32(64%) of respondents emphasized that there were security passwords on computers in their schools but only 4(8%) of respondents stressed that they did not have security passwords on computers in their schools. This clearly means that schools that have computers followed security practices by putting security passwords on their computers to prevent theft and possible intrusions. From Table 2 majority 34(68%) of respondents were neutral to the statement that vulnerability management measures were used in computers in their schools whilst very few 16(24%) of respondents also attested to the fact that vulnerability management measures were used in their schools. The result above implies that some of the senior high schools in the Keta Municipality were following computer security practices whilst other schools did not. This could also be attributed to majority of teachers using their personal computers in the school and don't see why they should be vulnerable if using their personal computer. Table 2 shows that majority 20(40%) of respondents emphasized that intrusion detective system was not used on computers in their schools to detect network attack whilst 24(48%) of respondents think otherwise were neutral. It is evidenced from the data above that computers in some of the senior high schools are not protected and therefore exposed to network attacks and even to hacker's attack. Also, it been established in Table 2 that majority 35(70%) of respondents attested to the fact that network security protocols are enforced in the school whilst only 5(10%) of respondents disagreed. This clearly indicated that network security protocols are enforced in some of the senior high schools in the Keta Municipality. Moreover, it been established in Table 2 that majority 39(78%) of respondents attested to the fact that computers are used for 70% during teaching and learning in the school whilst only 9(18%) of respondents disagreed. This clearly indicated that computers are used for 70% during teaching and learning in some of the senior high schools in the Keta Municipality. Also, it been established in Table 3 that all 50(100%) of respondents attested to the fact that there is no hacking attacks occuring with the computers in the school. This clearly indicated that there is no hacking attacks occuring with the computers in some of the senior high schools in the Keta Municipality.

Table 3 establishes that majority 7(70%) of respondents attested to the fact that there is Antivirus is installed on computers in my school whilst only 1(10%) of respondents disagreed and 2(20%) were neutral. This clearly indicated that computer security practices were strictly followed in some of the senior high schools in the Keta Municipality. As indicated in Table 3 that majority 7(70%) of respondents said that they did not transfer data from one computer to another but

**Table 1. Computer security practices by student**

| Variable | SA n (%) | A n (%) | N n (%) | D n (%) | SD n (%) |
|---|---|---|---|---|---|
| Computers in my school are networked. | 3(7.5) | 16(40) | 1(2.5) | 7(17.5) | 13(32.5) |
| there is password on computers in my school | 7(17.5) | 12(30) | 3(7.5) | 5(12.5) | 13(32.5) |
| I use computers in my school with permission | 23(57.5) | 12(30) | 2(5) | - | 3(7.5) |
| I easily download software's and files from the internet onto the computers in the school | 5(12.5) | 6(15) | - | 7(17.5) | 22(55) |
| I can install any program of my choice on the school's computers. | 4(10) | 4(10) | 1(2.5) | 19(47.5) | 12(30) |
| There is antivirus on computers in my school | 5(12.5) | 16(40) | 8(20) | 8(20) | 3(7.5) |
| Antivirus on the school's computers is often updated | 5(12.5) | 10(25) | 14(35) | 8(20) | 3(7.5) |
| There are security browsers on computers in my school | 1(2.5) | 7(17.5) | 11(27.5) | 13(32.5) | 8(20) |
| I use flash drives on computers in my school | - | 11(27.5) | 3(7.5) | 14(35) | 12(30) |
| Network security protocols are enforced in my school | 13(32.5) | 16(40) | 1(2.5) | 7(17.5) | 3(7.5) |
| Computers are used for 70% during teaching and learning in my school | 10(25) | 14(35) | 8(20) | 3(7.5) | 5(12.5) |
| Hacking attacks occur with the computer in my school | - | - | 1(2.5) | 7(17.5) | 32(80) |
| There is always a teacher or an instructor whenever we want to use the computers in the lab. | 47.5 | 47.5 | - | 2(5) | - |
| There are code of conduct guiding computer usage in my school | 11(40) | 16(42.5) | 2(5) | 3(7.5) | 2(5) |

*Source: Field Survey, (2019)*

**Table 2. Computer security practices by teachers**

| Variable | SA n (%) | A n (%) | N n (%) | D n (%) | SD n (%) |
|---|---|---|---|---|---|
| Antivirus is used on computers in my school | 24(48) | 18(36) | 4(8) | 4(8) | - |
| there is security password on computers in my school | 22(44) | 10(20) | 14(28) | 4(8) | - |
| There is firewall on computer system to prevent hackers in my school. | 4(8) | 8(16) | 26(52) | 8(16) | 4(8) |
| There is intrusion detective system to detect network attack | - | 6(12) | 24(48) | 12(24) | 8(16) |
| Vulnerability management measures are used in computers in my school | - | 8(16) | 34(68) | 4(8) | 4(8) |
| Original software with activation keys is installed on the computers | 8(16) | 10(20) | 28(56) | 4(8) | - |
| Software are updated regularly | 4(8) | (8)16 | 28(56) | 10(20) | - |
| There are special computers for teachers. | | | 8(16) | 16(32) | 26(52) |
| Students can install any software on their own without any administrative login. | - | 4(8) | 6(12) | 14(28) | 26(52) |
| teachers have individual logins to the school management system | 4(8) | 8(16) | 14(28) | 14(28) | 10(20) |
| Network security protocols are enforced | 23(46) | 12(24) | 5(10) | 10(20) | - |
| Computers are used for 70% during teaching and learning | 22(44) | 17(34) | 2(4) | 4(8) | 5(10) |
| Hacking attacks occur with the computer in the school | - | - | - | 12(24) | 38(76) |
| Teachers can easily download software's and files from the internet onto the computers in the school. | - | 12(24) | 10(20) | 18(36) | 10(20) |
| I sometimes give my login credentials to students. | - | - | - | 24(48) | 26(52) |
| I sometimes give my login credentials to colleague teachers. | - | 8(16) | 16(32) | 14(28) | 12(24) |
| Teachers allow students to enter marks into the school management system. | 4(8) | 4(8) | 6(12) | 8(16) | 28(56) |

*Source: Field Survey, (2019)*

**Table 3. Computer security practices by administrator and account clerk**

| Variable | SA n (%) | A n (%) | N n (%) | D n (%) | SD n (%) |
|---|---|---|---|---|---|
| Antivirus is installed on computers in my school | - | 7(70) | 2(20) | - | 1(10) |
| Software's on my computer are often updated regularly | - | 1(01) | 1(10) | 6(60) | 2(20) |
| There is security password on computers in my school | 2(20) | 5(50) | - | 3(30) | - |
| There is intrusion detective system to detect network attack | - | - | - | 5(50) | 5(50) |
| I transfer data from one computer to another | 1(10) | 5(50) | - | 1(10) | 3(30) |
| Original software with activation keys are installed on the computers. | 2(20) | - | 2(20) | 4(40) | 2(20) |
| I have experienced hacking or attack on my computer | - | - | 1(10) | 2(20) | 7(70) |
| I ever given my password to a friend to log in on my behalf | 1(10) | 2(20) | 2(20) | - | 2(20) |
| Teachers or students are able to log into your computer. | - | 2(20) | 2(20) | 4(40) | 2(20) |
| I often download software's, videos, files from the internet | 4(40) | - | - | 4(400 | 2(20) |
| I do open strange mails and download its content. | - | - | 3(30) | 6(60) | 1(10) |
| Network security protocols are enforced | 5(50) | 3(30) | 1(10) | 1(10) | - |
| Hacking attacks occur with the computer in the school | - | - | - | 4(40) | 6(60) |
| There are property markings on computers in my school. | 2(10) | 1(10) | - | 4(40) | 3(30) |

*Source: Field Survey, (2019)*

only 4(40%) of respondents confirmed that they did transfer data from one computer to another. Table 3 also shows that majority 6(60%) of respondents indicated that they have security passwords on their computers whilst very few 4(40%) of respondents established that they did not have security passwords on their computers. It could be observed from the data above that some of administrators and account clerks in the senior high schools in the Keta Municipality were strictly following the computer security practices whereas some were also not on top of computer security issues in some of the senior high schools in the Municipality. Moreover, it been established in Table 3 that majority 8(80%) of respondents attested to the fact that network security protocols are enforced in the school whilst only 1(10%) of respondent disagreed. This clearly indicated that network security protocols are enforced in some of the senior high schools in the Keta Municipality. Also, it been established in Table 3 that all 10(100%) of respondents attested to the fact that there is no hacking attacks occuring with the computers in the school. This clearly indicated that there is no hacking attacks occuring with the computers in some of the senior high schools in the Keta Municipality.

From Table 3, it is established that 7(70%) of respondents unanimously agreed to the fact that antivirus is installed on computers in their offices whilst 1(10) disagree. According to Schneier [18], organizations such as schools and banks must inevitably come to terms with new modes of communication as well as new technological equipment and machinery that deal with topics such as result recording, completing and updating school records, and money. According to Viega & Mcgraw [2], there is a natural push on schools to adapt to new technology such as intrusion detective instruments and tools in their computer systems. The same impulse drives teachers and account clerks who use computers in their everyday lives attach importance to the use of intrusion detective systems in their computers. Landwehr, Bull & McDermott [19], emphasized that the defence tactics all organisations and schools are engaging to protect against the possibility of a malware today is simply inadequate. Trusted sessions, such as those between a user and a school, can be hacked or hijacked in a variety of ways. The security response to these emerging threats is shaky and ineffective. It's tentative in the sense that new threats are identified on a regular basis, and we're still far from having a complete understanding of the web application threat spectrum. Computer security is a difficult problem that requires a more complex solution than is currently available. However, one of the ways of ensuring this sophistication in data protection is by introducing artificial intelligence technology in intrusion detection systems. Artificial intelligence technology facilitates and ensures effective protection of systems. Studies further corroborates this finding by stating that artificial intelligence could potentially improve radically the performance of intrusion detection systems, which directly alerts users or networks of an impending or ongoing system attacks [20]. What is less obvious is how to operationalize this idea in order to protect computers from attack. It is important to acknowledge that the use of artificial intelligence practice everywhere in computer security must however be strictly followed and adhered to in order to address cyber-attacks as shown in Table 3. To adequately secure the increasing amount of capability and complexity in computer security, future artificial intelligence systems involved in computer security would have to be far more advanced than anything we can fathom today [21].

In conclusion intrusion detective system such as artificial intelligence indeed needs to be provided in senior high schools to protect confidentiality, authentication, integrity, nonrepudiation, access control, and properties of senior high schools and organisations. *According to Klein, Roff, & Hehir [11], the most important thing to remember when it comes to computer security is to be careful of what websites you visit, what links you click on, what you enter your information into, and what you download. Antivirus software comes pre-installed on the majority of computers.* For example, Windows 8 and 10 include Windows Defender, which is sufficient for the majority of users. As shown in Table 3, the study recommended Avast because it has been one of the most highly rated antivirus products for years, it does not slow down your system, and it is absolutely free. Vulnerability management, according to Cheswich & Bellon [22], is the process of discovering, remediating, or minimizing vulnerabilities, particularly in software and hardware. Vulnerability management is crucial to network and computer security. Vulnerabilities can be found with a vulnerability scanner, which examines a computer system for known flaws such open ports, unsecured software configuration, and malware susceptibility. In addition to vulnerability

scanning, many companies use professional security auditors to conduct frequent penetration testing on their systems to find flaws. As evidenced by Table 2 above, this is a contractual necessity in some industries.

## 4. CONCLUSION

A computer security practice is indispensable tool and measure to promote and improve computer use in all schools across the nation. A computer security practice is a serious issue affecting effective teaching and learning and school management in senior high schools nowadays in Ghana in general and the Keta Municipality in particular and indeed need a pragmatic and urgent attention. Computer security practices should be enforced and applied in senior high schools in the Keta Municipality to protect schools' files, documents, personnel records, leakage of examination questions, and change of examination results, duplication of files, vital properties and documents of the schools from being hacked and leaked to the public. It is therefore necessary to supply well-functioning computers that are protected against threat in senior high schools if indeed security of file document and protection of school's data and information are taken serious. To achieve as a result, strict computer security practices and measures must be put in place in all senior high schools in the Keta Municipality to prevent and protect school files, document and vital properties of the school from hackers and attackers.

## 5. RECOMMENDATIONS

The study recommends that adequate and functional computers should be provided in senior high schools in the Keta Municipality to promote effective teaching and learning. Also, ICT teachers should be abreast with maintenance of the computers. Furthermore, strict measures should be put in place to protect school files and documents from hackers and theft. There should be code of ethics to regulate computer use and intrusion detective devices on computers to prevent unlawful logging into school management system. Moreover, further studies should be done on this study in different geographical area to confirm or contrast with the findings of the study. Also, future studies can look into the trend in computer usage at the basic schools

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES


1. Ferreira FA, Castro C. Medical tourism in portugal – A potential niche market. In: Rocha Á., Abreu A, de Carvalho J, Liberato D, González E, Liberato P. (eds) Advances in Tourism, Technology and Smart Systems. Smart Innovation, Systems and Technologies. 2020;171. Springer, Singapore. Available:https://doi.org/10.1007/978-981-15-2024-2_53
2. Viega, McGraw. Building secure software: How to avoid security problems the right way; 2001.
3. Hoglund, McGraw. Exploiting software, how to break code. Boston;2004.
4. Algarni S. Cybersecurity Attacks: Analysis of "WannaCry" attack and proposing methods for reducing or preventing such attacks in future. In: Tuba M, Akashe S, Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing. 2021;1270. Springer, Singapore. Available:https://doi.org/10.1007/978-981-15-8289-9_73
5. Chisita CT, Chiparausha B. An Institutional Repository in a Developing Country: security and Ethical Encounters at the Bindura University of Science Education, Zimbabwe. New Review of Academic Librarianship, 2021;27(1):130–143. Available:https://doi.org/10.1080/13614533.2020.1824925
6. Amran A, Zaaba ZF, Singh MKM. Habituation effects in computer security warning. Information Security Journal: A Global Perspective. 2018;27(4):192–204. Available:https://doi.org/10.1080/19393555.2018.1505008
7. Yadav T, Sadhukhan K. Identification of Bugs and Vulnerabilities in TLS Implementation for Windows Operating System Using State Machine Learning. In: Thampi S, Madria S, Wang G, Rawat D, Alcaraz Calero J. (eds) Security in Computing and Communications. SSCC 2018. Communications in Computer and Information Science. 2019;969. Springer, Singapore. Available:https://doi.org/10.1007/978-981-13-5826-5_27

8. Al-khatib AA, Hassan MA. Managing computer security, risk analysis and threat using iso 31000:2009: Case study at seiyun community college, Yemen. International Journal of Network Security. 2019;21(4):566–575.
9. Anderson. Security engineering: A guide to building dependable distributed systems. John Wiley and Sons, New York; 2001.
10. Richardson MD, Lemoine PA, Stephens WE, Waller RE. Planning for cyber security in schools: The human factor. Educational Planning. 2020;27(2):23–39.
11. Klein D, Roffi A, Hehir J. Cyber security and schools: A learning opportunity;2015.
12. Howard M, LeBlanc. *Writing secure code*. Microsoft press, Redmond, WA;2003.
13. Wang Q, Lu P. Research on application of artificial intelligence in computer network technology. International Journal of Pattern Recognition and Artificial Intelligence. 2019;33(5).
Available:https://doi.org/10.1142/S0218001419590158
14. Haner JK, Knake RK. Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. Journal of Cybersecurity. 2021;00(0):1–15.
15. Geer B, Rebecca B, Peter G, Perry M, Charles P. Cyber insecurity: The cost of. 2003;302.
16. Li C, Gaudiot JL. Securing computer systems through cyber attack detection at the hardware level. University of California, Irvine; 2020.
17. Campbell S, Greenwood M, Prior S, Shearer T, Walkem K, Young S, Walker K. Purposive sampling: complex or simple? Research case examples. Journal of Research in Nursing. 2020;25(8):652–661.
Available:https://doi.org/10.1177/1744987120927206
18. Schneier. *Secrets and lies*. New York; 2000.
19. Landwehr, Bull, McDermott. A Taxonomy of computer program security flaws, with examples. Technical Report NRL/FR/5542—93/9591, United States Navy, Naval Research Laboratory; 1993.
20. Du X, Hargreaves C, Sheppard J, Anda F, Sayakkara A, Le-Khac NA, Scanlon M. SoK: exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020;(46):1–10.
Available:
https://doi.org/10.1145/3407023.3407068
21. Jurjens. Towards secure systems development with UMLsec. Proceedings of FASE'01. Springer Lecture Notes in Computer Science; 2001.
22. Cheswich, Bellon. *Firewalls* and internet security. The very first edition of a classic security tome;1994.




*Peer-review history:*
*The peer review history for this paper can be accessed here:*
*http://www.sdiarticle4.com/review-history/69679*